



## Compliance Component

### DEFINITION

<i>Name</i>	Host-Based Intrusion Detection Systems (HIDS)
<i>Description</i>	Host-Based Intrusion Detection Systems (HIDS) operate on information collected from within an individual computer system. This vantage point allows HIDS to analyze activities to determine exactly which processes and users are involved in an attack on a particular system or host. HIDS can see the outcome of an attempted attack, as they can directly access and monitor the data files and operating system processes targeted by the attack.
<i>Rationale</i>	<p>The first step in delivering an efficient and secure intrusion protection strategy is accurately detecting all possible threats. To achieve this goal, multiple detection methods including HIDS should be employed to ensure comprehensive coverage.</p> <p>The failure to secure any State of Missouri host system with HIDS puts agencies at a much greater risk of loss. A single attack can cost millions of dollars in time spent recovering from the attack and liability for compromised data and hardware. The damage from an attack to State of Missouri services can also include inconvenience to citizens and the loss of public confidence.</p>
<i>Benefits</i>	<ul style="list-style-type: none"> <li>• HIDS can detect attacks that cannot be seen by a Network-Based IDS since they monitor events local to a host.</li> <li>• HIDS can often operate in an environment where network traffic is encrypted.</li> <li>• HIDS are unaffected by switched networks.</li> <li>• HIDS can detect, and in some cases prevent, attacks that involve software integrity breaches, such as Trojan Horses.</li> <li>• HIDS have the ability to monitor local files for any changes or modifications.</li> <li>• HIDS can see the outcome of an attempted attack since they can directly access and monitor the data files and operating system processes targeted by the attack.</li> </ul>

### ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Technical Controls
<i>List the Technology Area Name</i>	Intrusion Detection Systems
<i>List Product Component Name</i>	

### COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

## COMPLIANCE DETAIL

### **General HIDS Requirements**

- Administrators shall be trained on the IDS before implementation. Despite vendor claims of ease of use, training and/or experience are absolutely necessary to manage any IDS.
- It is preferred to have the HIDS controlled directly from a central location(s). However, the HIDS may be agent-based where response decisions are made at the host.
- IDS administrators shall be able to create or change policies easily.

### **HIDS Deployment Requirements**

- HIDS shall be deployed in conjunction with Network-Based IDS to fully protect the system.
- It is recommended that organizations install the Network-Based IDS first, followed by the HIDS installation on critical servers. Once administrators are familiar with the HIDS, it may be installed on the remainder of the organization's hosts.
- HIDS shall be installed on any host where sensitive or critical information is stored.
- It is preferred to install IDS Management software on a separate system from the target host being monitored.
- It is preferred to have the HIDS use an agent-manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents.
- It is preferred that host agents poll the manager at periodic intervals for policy changes or new software updates.

### **HIDS Analysis Requirements**

- HIDS shall utilize information from operating system audit trails and system logs.
- HIDS shall have easy-to-use tools to analyze the logs.
- HIDS shall detect, and preferably prevent, the following:
  - System scanning (probing the target with different kinds of packets to garner information about the system, such as topology, active hosts, operating systems and software in use),
  - Denial of Service (DoS) (slow or shut down targeted systems or hosts), and
  - Penetration (unauthorized acquisition and/or alteration of system privileges, resources, or data).
- HIDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may also include Anomaly Detection (abnormal, unusual behavior) components.
- Administrators shall follow a schedule for checking the results of the HIDS to ensure attackers have not modified the system.

*State the Guideline, Standard or Legislation*

### **HIDS Response Requirements**

- HIDS shall respond in real-time.
- It is preferred that HIDS provide active responses to intrusions by:
  - Collecting additional information:
    - Turning up the number of events logged, or
    - Capturing all packets, not just those targeting a particular port or system.
  - Changing the environment:
    - Terminating the connection, or
    - Reconfiguring routers and firewalls to:
      - Block packets from the intruder's IP address,
      - Block network ports, protocols or services, or
      - Sever all connections that use certain network interfaces.
- HIDS administrators shall work closely with router and firewall administrators when creating rules for routers and firewalls to ensure intruders cannot abuse the feature to deny access to legitimate users.
- HIDS may provide passive responses requiring subsequent human action to intrusions by:
  - Generating alarms and notifications with popup windows, cellular phones, pagers and email, or
  - Reporting alarms and alerts using SNMP traps and plug-ins to central network management consoles.
- All HIDS communications shall be secure and use encrypted tunnels or other cryptographic measures
- HIDS shall create output with the following information for each intrusion detected:
  - Time/date
  - Sensor IP address
  - Specific attack name
  - Source and destination IP addresses
  - Source and destination port numbers
  - Network protocol used
  - Description of the attack type
  - Attack severity level
  - Type of loss expected
  - Type of vulnerability exploited
  - Input validation (buffer overflow or boundary condition)
  - Access validation (faulty access control mechanism)
  - Exceptional condition
  - Environmental (unexpected interaction with an application and the operating system or between two applications)
  - Host Configuration

	<ul style="list-style-type: none"> <li>o Race (delay between the time a system checks to see if an operation is allowed and the time it performs the operation)</li> <li>o Design</li> <li>o Software types and versions vulnerable</li> <li>o Patch information to counter the attack</li> <li>o References to advisories about the attack or vulnerability</li> </ul> <ul style="list-style-type: none"> <li>• It is preferred that HIDS reports combine redundant attack entries and make attacks of highest importance stand out.</li> </ul>	
<i>Document Source Reference #</i>	<p>NIST SP 800-31_(<a href="http://www.csrc.nist.gov/publications/nistpubs">www.csrc.nist.gov/publications/nistpubs</a>) Intrusion Detection Systems (IDS),</p> <p>NIST SP 800-18 (<a href="http://www.csrc.nist.gov/publications/nistpubs">www.csrc.nist.gov/publications/nistpubs</a>) CERT Guide to System and Network Security Practices (<a href="http://www.cert.org/security-improvement/">www.cert.org/security-improvement/</a>)</p>	
<b>Standard Organization</b>		
<i>Name</i>	<i>Website</i>	
<i>Contact Information</i>		
<b>Government Body</b>		
<i>Name</i>	<p>National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)</p> <p>CVE Vulnerability Search on ICAT Metabase</p>	<p><i>Website</i></p> <p><a href="http://csrc.nist.gov/">http://csrc.nist.gov/</a></p> <p><a href="http://icat.nist.gov/">http://icat.nist.gov/</a></p>
<i>Contact Information</i>	<a href="mailto:inquiries@nist.gov">inquiries@nist.gov</a>	
<b>KEYWORDS</b>		
<i>List all Keywords</i>	Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes	
<b>COMPONENT CLASSIFICATION</b>		
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>	
<b>Rationale for Component Classification</b>		
<i>Document the Rationale for Component Classification</i>		
<b>Conditional Use Restrictions</b>		
<i>Document the Conditional Use Restrictions</i>		
<b>Migration Strategy</b>		
<i>Document the Migration Strategy</i>		
<b>Impact Position Statement</b>		
<i>Document the Position Statement on Impact</i>		

### CURRENT STATUS

*Provide the Current Status)*

*In Development*

*Under Review*

*Approved*

*Rejected*

### AUDIT TRAIL

<i>Creation Date</i>	04/03/2003	<i>Date Accepted / Rejected</i>	05/14/2003
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			